



lyit

Institiúid Teicneolaíochta Leitir Ceannainn  
Letterkenny Institute of Technology

# *User Attitudes to BYOD Security & the Cloud*

Authors: R G Lennon

Presented by: Valerie Smyth



# Background

- Letterkenny Institute of Technology (LYIT) is moving towards the support of 'Bring your own Devices'.
  - Laptops
  - Mobile phones
  - Table pc's
  - External disk drives
  - E-readers
- In the early research it was found that users placed little concern on the security of these devices.



lyit

Institiúid Teicneolaíochta Leitir Ceanainn  
Letterkenny Institute of Technology

# BYOD

- Bring Your Own Device (BYOD) is gaining popularity with students as it enables them to continue working from home.
- BYOD integrates nicely with the Cloud and Virtual Learning Environments.
- BYOD drastically reduces costs to LYIT in providing hardware/software for the students.



lyit

Institiúid Teicneolaíochta Leitir Ceanainn  
Letterkenny Institute of Technology

# Increased BYOD usage

- The number of unauthenticated devices, such as mobile phones and other smart devices has increased by an average of 65% per month since September 2011.
  - 47% are laptops/tablets
  - 39% are mobile phones
- 70% of survey respondents said that their home wireless network went down at least once per month.



lyit

Institiúid Teicneolaíochta Leitir Ceanaínn  
Letterkenny Institute of Technology

# User Security

- The risks in connecting to the wireless network is well established.
- BYOD owners may connect to resources held on the Cloud using valid login details but over an unsecured network such as those found in internet cafés.



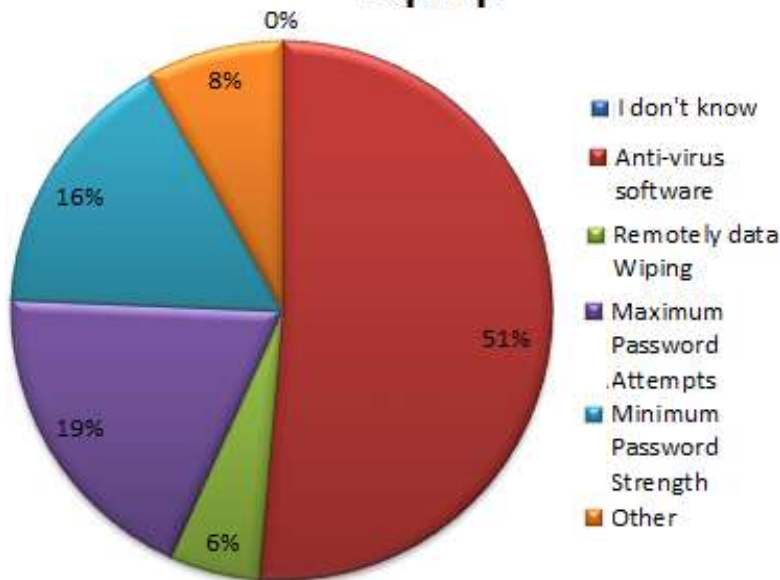
lyit

Institiúid Teicneolaíochta Leitir Ceanainn  
Letterkenny Institute of Technology

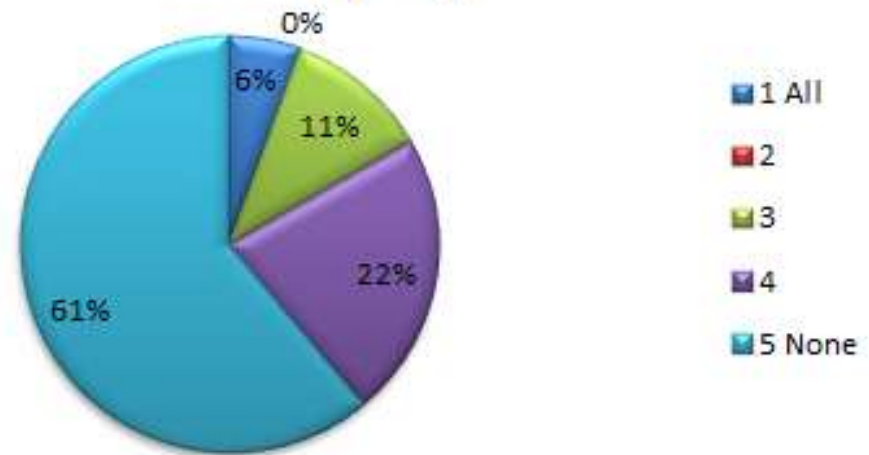
# BYOD Security Knowledge

- When questioned about the security of their device many users were unaware of any security other than Anti-virus software.

Security Features installed on the Laptop



Proportion of Files Encrypted on the Laptop.



# Have you been Hacked?

- When asked if they had ever been hacked 71% of the respondents indicated that they were not.
- However, when further interviews were conducted it became apparent that some of respondents had been hacked but were unaware of techniques to assess this situation



lyit

Institiúid Teicneolaíochta Leitir Ceanainn  
Letterkenny Institute of Technology

# BYOD & the Cloud

- Using the BYOD device to access information stored on a virtualised service is essential to increased productivity.
- However separating personal data from work related data is a concern.
- If the mobile device is breached notification (and possible remote wiping) must be carried out within a minimum time period.



lyit

Institiúid Teicneolaíochta Leitir Ceanainn  
Letterkenny Institute of Technology



# EU Laws

- Electronic Communications Network.
  - The BYOD device may be considered part of the infrastructure to support communications.
- Confidentiality of communications may be breached on the BYOD device by Mobile Management services.
- Article 13 of Directive 2000/13/EC refers to caching of data on a communications network.



# Summary

- BYOD is inevitable.
- Resources will be held on the Grid and on the Cloud for access via BYOD devices.
- Users are generally unaware of the risks in using BYOD.
- Managers need to regulate BYOD use and data transfer.
- EU law is progressing to encompass these themes but they are not finalised yet.



lyit

Institiúid Teicneolaíochta Leitir Ceanainn  
Letterkenny Institute of Technology

# Conclusions

- Education of BYOD users is key.
- BYOD to connect to resources on the Grid and/or on the Cloud may be defined under new laws.
- Each case must be separately evaluated.



lyit

Institiúid Teicneolaíochta Leitir Ceanaínn  
Letterkenny Institute of Technology



lyit

Institiúid Teicneolaíochta Leitir Ceanainn  
Letterkenny Institute of Technology

Thank you.

Questions?

Valerie Smyth

